IN THE SPECIFICATION

Please amend paragraph [0004] beginning on page 3, as follows:

[0004] Occasionally the situation arises where the VPN client unit wants to temporarily exercise its granted VPN access authority in another VPN client unit. Further, in the case where the VPN client unit (A) is inside an NAT (Network Address Translation) segment or where it is a portable miniature device of severely limited power requirements, it is not proper to directly establish an encrypted channel for communication with the VPN gateway unit. In this instance, it is typical that another VPN client unit (D), which possesses the function of gateway from the NAT segment concerned to the Internet, takes the charge of establishing a tunnel to the VPN gateway. In this case, access control needs to be conducted ~~effected~~ for the VPN client unit (A), not for the VPN client unit (D). Thus, when the VPN client unit granted the access authority differs from the VPN client unit from which the tunnel starts, a mechanism for delegating authority is indispensable.

Please amend paragraph [0008] beginning on page 5, as follows:

[0008] Patent document 4, non-patent document 1, non-patent document 2 and non-patent document 3 all set forth methods of dynamic setting/posting of the configuration management information by such tunneling protocols as IPsec, PPP, L2TP, and the like. The present invention also makes an assumption that the function corresponding to the above-mentioned dynamic setting/posting is performed in the set-up phase of various tunnel protocols between the VPN client unit and the VPN gateway unit. But, according to the conventional systems, user authentication or access control and the dynamic setting/posting of the above-mentioned configuration management information are carried out as a single, integral operation at the time of tunnel set-up; in contrast thereto, according to the present invention, the user authentication and the access control are performed in a mediating apparatus to allow the VPN client unit and the VPN gateway unit to share a common secret, which is used to set up a tunnel between the VPN client unit and the VPN gateway unit, and then the configuration management information about the tunnel is dynamically set/posted from the VPN gateway unit. Besides, the VPN client unit A delegates the tunnel protocol processing for encrypted communication to another reliable VPN client unit D, by which it is possible to make a check of the access authority in the mediating apparatus for the source unit B. According to management convenience, part of the configuration management information on the tunnel, information for routing to the tunnel, or similar information about network operation, may be sent from the mediating apparatus to the VPN client unit. In this instance, the configuration management information sent from the mediating apparatus is set before or after tunnel setup in accordance with the kind of information. As an authentication and a certificate issuing method using a public key, there is proposed an SPKI (Simple Public Key Infrastructure) scheme (for example, non-patent document 4, and non-patent document 5), but it is not clear how to apply the scheme to the remote-access VPN.

Patent document 1: Japanese Patent Application Kokai Publication No.2001-292135

Patent document 2: Japanese Patent Application Kokai Publication No.2002-271309

Patent document 3: Japanese Patent Application Kokai Publication No.2003-18163

Patent document 4: Japanese Patent Application Kokai Publication No.2001-160828

Non-patent document 1: B. Patel, B. Aboba, S. Kelly, V. Gupta, "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Model," [online], published January, 2003. RFC3456, Internet Engineering Task Force, [Retrieved March 17, 2003], Internet ~~URL:http://www.ietf.org/rfc/rfc3456.txt~~ www.ietf.org/rfc/rfc3456.txt

Non-patent document 2: IPCP (RFC-1332)

Non-patent document 3: EAP (RFC-2284)

Non-patent document 4: C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, “SPKI Certificate Theory,” [online], published September 1999, RFC2693, Internet Engineering Task Force, Internet ~~URL:http://www.ietf.org/rfc/rfc2693.txt~~ www.ietf.org/rfc/rfc2693.txt

Non-patent document 5; C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, “Simple Public Key Infrastructure <draft-ieft-spki-cert-structure-0.6.txt>” [online], published July 26, 1999, Internet Engineering Task Force, ~~InternetURL:http://world.std.com/~cme/spki.txt~~ Internet world.std.com/~cme/spki.txt

Please delete the section heading on page 7, line 9 and insert therefor a new section heading, as follows:

DISCLOSURE OF THE INVENTION

Please amend paragraph [0010] beginning on page 7, as follows:

[0010] According to the present invention, there is provided a remote-access VPN mediating method in a system wherein: a virtual private network, hereinafter referred to as VPN, client units and a VPN gateway unit are connected to an IP network; communication units are connected to a local area network placed under the management of the VPN gateway unit; and a remote-access VPN by a tunneling protocol is implemented between an arbitrary one of VPN client units and the VPN gateway unit connected to said IP network and an arbitrary one of the communication units connected to the local area network placed under the management of the VPN gateway [[unit;]] unit, said method comprising the steps of:

(a) sending an access control list containing information indicative of a private IP address assigned to said communication unit to a mediating apparatus on said IP network from said VPN gateway unit;

(b) storing said access control list by said mediating apparatus in correspondence to said VPN gateway unit;

(c) retrieving an IP private address corresponding to said VPN gateway unit in response to a request from said VPN client unit, acquiring the private IP address of the corresponding communication unit from said access control list, sending the acquired private IP address to said VPN client unit, sending the IP address of said VPN client unit to said VPN gateway unit, generating mutual authentication information for setting up an authenticated encrypted tunnel between said client VPN unit and said gateway unit, and sending said mutual authentication information to both of said VPN client unit and said gateway unit; and

(d) setting up said authenticated encrypted tunnel between said VPN client unit and said gateway unit by use of said mutual authentication information, and implementing remote access through said encrypted tunnel by use of the private IP address of said communication unit.

Please amend paragraph [0011] beginning on page 8, as follows:

[0011] According to the present invention, there is provided a remote-access VPN mediating apparatus which is built on an IP network to implement a remote-access VPN in a system wherein: VPN client units and a VPN gateway unit are connected to the IP network; communication units are connected to a local area network placed under the management of said VPN gateway unit; and a remote-access VPN by a tunneling protocol is implemented between an arbitrary one of said VPN client units and said VPN gateway unit connected to said IP network and an arbitrary one of said communication units connected to said local area network placed under the management of said VPN gateway [[unit;]] unit, said apparatus comprising:

ACL storage means for storing an access control list, hereinafter referred to as ACL, sent from said VPN gateway unit and containing information indicative of the private IP address assigned to said communication unit;

authentication/access authorization control means for authenticating said VPN client unit and said gateway unit, and for executing access authorization control;

IP address acquiring means for referring to said access control list to acquire the private IP address assigned to said communication unit, and for searching a domain name server to acquire the IP address assigned to said VPN gateway unit;

authentication information generating means for generating mutual authentication information for setting up an encrypted tunnel between said VPN client unit and said VPN gateway unit; and

communication means for sending the IP address of said VPN gateway unit, the private IP address of said communication unit and said mutual authentication information to said VPN client unit, and for sending the IP address of said PN client unit and said mutual authentication information to said VPN gateway unit.

Please amend paragraph [0031] beginning on page 22, as follows:

[0031] In the case of delegating to the VPN client unit (D) 102 the authority for retrieving the IP address of the VPN gateway unit (B) 103, the VPN client unit (A) 101 sends a certificate CERT to the VPN client unit (D) 102 by the SPKI scheme (step S6). The VPN client unit ~~(C)~~ (D) 102 sends its public key PUBLICKEY_D and the certificate CERT, and the public key PUBLICKEY_B (or its hash value HASH_B) to the mediating apparatus (S) 104 to make a request for retrieval of the IP addresses of the VPN gateway unit (B) 103 and the communication unit (C) (step S7). The mediating apparatus (S) 104 exercises the access authorization control for the VPN client unit (D) 102 by the SPKI scheme, and in the case of authorizing access, the mediating apparatus searches the domain name server ~~(DCS)~~ (DNS) 105 to obtain the IP address IPADDRESS_B assigned to the VPN gateway unit (B) 103 (step S8). Then the mediating apparatus (S) 104 refers to the access control list (ACL) to obtain the private IP address IPADDRESS_C of the communication unit (C) 111 connected to LAN 110 that is placed under the management of the VPN gateway unit (B) 103. Then the mediating apparatus (S) 104 generates a common key KEY_DB that is used for mutual authentication between the VPN gateway unit (B) 103 and the VPN client unit (D) 102. Then the mediating apparatus (S) 104 uses the public key PUBLICKEY_D of the VPN client unit ~~(C)~~ (D) 102 to encrypt the communication channel between the mediating apparatus (S) 104 and the VPN client unit (D) 102, and sends the IP addresses IPADDRESS_B and IPADDRESS_C and the common key KEY_DB to the VPN client unit (D) 102 over the encrypted communication channel (step S9). Then the mediating apparatus (S) 104 uses the public key PUBLICKEY_B of the VPN gateway unit (B) 103 to encrypt the communication channel between the mediating apparatus (S) 104 and the VPN gateway unit (B) 103, and sends the IP address IPADDRESS_D and the common key KEY_DB to the VPN gateway unit (B) 103 (step S10). Thus the VPN client unit (D) 102 and the VPN gateway unit (B) are enabled to carry out secure communications between them by use of the common key KEY_DB.

Please amend paragraph [0057] beginning on page 39, as follows:

[0057] Next, a description will be given, with reference to Fig. 13, of the general outline of the operation of the Fig. 12 embodiment. At the time of entering (storage) of the access control list (ACL), the VPN gateway unit (B) 103 sends the public key PUBLICKEY_B (or its hash value HASH_B) and the access control list (ACL) to the mediating apparatus (S) 104 ~~(step S21)~~ (step S1). The mediating apparatus (S) 104 stores the access control list (ACL) as the tables of Figs. 4A and 4B in association with the public key PUBLICKEY_B (or its hash value HASH_B). In the case of implementing the remote-access VPN from the VPN client unit (A) 101 to the communication unit (C) 111 via the VPN gateway unit (B) 103 in the IPsec tunnel mode, the VPN client unit (A) 101 sends the public key PUBLICKEY_A and the public key PUBLICKEY_B (or its hash value HASH_B) to the mediating apparatus (S) 104 to make a request for retrieval of the IP addresses of the VPN gateway unit (B) 103 and the communication unit (C) ~~111(step S22)~~ 111 (step S2).

Please amend paragraph [0058] beginning on page 39, as follows:

[0058] In the case where the authentication/access authorization control means 1042 executes the access authorization control for the VPN client unit (A) 101 by the PKI scheme for granting it access authorization, the mediating apparatus (S) 104 searches the domain name server (DNS) 105 and retrieves therefrom the IP address IPADDRESS_B assigned to the VPN gateway unit (B) 103 ~~(step S23)~~ (step S3). The mediating apparatus (S) 104 refers to the access control list (ACL) to obtain therefrom the private IP address IPADDRESS_C and attribute information ATTRIBUTE_A of the communication unit (C) 111 connected to the LAN 110 placed under the management of the VPN gateway unit (B) 103. Furthermore, the mediating apparatus (S) 104 generates the common key KEA_B that is used for authentication between the VPN client unit (A) 101 and the VPN gateway unit (B)

103. And, the mediating apparatus (S) 104 encrypts the communication channel between the mediating apparatus (S) 104 and the VPN client unit (A) 101, through which it sends the IP addresses IPADDRESS_B, IPADDRESS_C and the common key KEY_AB to the VPN client unit (A) 101 ~~(step S24)~~ (step S4). Moreover, the mediating apparatus (S) 104 encrypts the communication channel between the mediating apparatus (S) 104 and the VPN gateway unit (B) 103, through which it sends the IP address IPADDRESS_A, the attribute information ATTRIBUTE_A and the common key KEY_AB to the VPN gateway unit (B) 103 ~~(step S25)~~ (step S5).

Please amend paragraph [0084] beginning on page 52, as follows:

[0084] Those of pieces of information B), C) and D) in item (2) which are not dynamically posted from the VPN gateway unit (which pieces of information may be provided from either one of the mediating apparatus and the VPN gateway unit). The mediation processing in this embodiment is performed as described below. In the first place, the application issues, prior to communication, a DNS query request for querying about the IP address of the VPN gateway unit that offers a VPN service desired to access ~~(step S1)~~ (step S11). This request is captured once by the DNS query capture/proxy answer function part 1011, which refers to the mediation service management table 1014 to decide whether the request concerns the mediation service or not. If the request has nothing to do with the mediation service, it is regarded as an ordinary DNS request, then ordinary DNS processing is performed for the DNS server 105 to obtain the IP address from its answer, and ordinary connection processing is carried out using it ~~(step S2)~~ (step S12).

Please amend paragraph [0085] beginning on page 52, as follows:

[0085] If the DNS inquiry request concerns the mediation service, it is transferred to the mediation-service VPN client function part 1012 ~~(step S3)~~ (step S13). The mediation-service VPN client function part 1012 selects a predetermined mediation server according to the contents of the mediation service management table 1014 ~~(step S4)~~ (step S14), and performs mutual authentication using the mediation-service authentication information table 1015 ~~(step S5)~~ (step S15). Then the mediation-service VPN client function part sends the mediation request, referred to with respect to the above-described embodiment, to the mediating apparatus 104 ~~(step S6)~~ (step S2) and obtains its answer ~~(step S7)~~ (step S4). Based on this information, the mediation-service VPN client function part updates information such as the VPN gateway addresses and common keys in the tunneling/protocol configuration management table 1016 ~~(step S8)~~ (step S16) and, if a predetermined tunnel is not set up yet, it sends a tunnel set-up request to the tunneling/protocol 1013 ~~(step S9)~~ (step S17).

Please amend paragraph [0086] beginning on page 53, as follows:

[0086] The tunneling/protocol part 1013 refers to the tunneling/protocol configuration management table 1016 to identify the VPN gateway unit 103 that is the opposite side of the tunnel ~~(step S10)~~ (step S18), and sets up a tunnel for encrypted communications with the VPN gateway unit 103 by use of the common key set by the present mediation function ~~(step S11)~~ (step S19). Once the tunnel is normally set up, part of configuration management information, such as the private IP address of the VPN client unit 101, internal DNS and routing-related information, can be dynamically passed from the VPN gateway unit 103 by use of the method set forth in patent document 4, non-patent document 1, non-patent documents 2, or non-patent document 3. In this case, the tunneling/protocol part uses these pieces of information t update the tunneling/protocol configuration management table 1016 ~~(step S12)~~ (step S20), and sends an answer of tunnel set-up completion to the mediation-service VPN client function part 1012 ~~(step S13)~~ (step S21).

Please amend paragraph [0087] beginning on page 53, as follows:

[0087] When the set-up of the VPN tunnel is normally completed, the mediation-service VPN client function part 1012 sends the private IP address of the communication unit obtained in ~~step S7~~ step S4, as an answer to the DNS query, to the DNS query capture/proxy answer function part 1011 ~~(step S14)~~ (step S22). This answer is sent intact to the application that issued the DNS query ~~(step S15)~~ (step S23). The application conducts VPN communication via the set VPN tunnel ~~(step S16)~~ (step S24).

EMBODIMENT 4

Fig. 19 illustrates an example of the entire system configuration embodying the present invention. In this embodiment, assume that VPN client units 101 and 102 are used for a personnel division and an accounting division, and that they have public key hash values A1 and A2, respectively. Let it be assumed that the VPNs placed under the management of the VPN gateway unit 103 are a personal division VLAN 121 and an accounting division VLAN 122, and that the VPN gateway unit 103 is connected via an ethernet switch 123 to both of VLANs 121 and 122 by IEEE 802.IQ VLAN tag multiplexing. Further, assume that the mediating apparatus 104 has pre-uploaded thereto the access control list (ACL) shown in Fig. 20 for the VPN gateway unit 103. In this ACL it is declared that the VPN client unit 101 having a public key of hash value HASH_A1 has attribute information "(VLAN Personal Division VLAN)", whereas the VPN client 102 having a public key of hash value HASH_A2 has attribute information "(VLAN Personnel Division VLAN)".

Please amend paragraph [0088] beginning on page 54, as follows:

[0088] Fig. 21 illustrates the functional configuration of the VPN gateway unit 103 in this embodiment. The VPN gateway unit 103 ~~102~~ is provided with: a mediation-service VPN gateway function part 1031 that performs communications with the mediating apparatus 104 and processing therefor; a tunneling/protocol part 1032 that terminates tunnels from multiple VPN client units; a filtering/VLAN multiplex function part 1033 that stores data packets extracted from the tunnels in predetermined VLANs in VPNs and filters out those of packets input to and output from the tunnels which raise security concerns. Furthermore, there are provided: a mediation service management table 1034 having information necessary for connection with the mediating apparatus 104; a mediation-service authentication information table 1035 for authentication with the mediating apparatus 104; a tunneling/protocol configuration management table 1036 holding configuration management information on tunnels to the VPN client units 101 and 102; and VLAN configuration management table 1037 holding configuration management information on each VLAN placed under the management of the VPN gateway unit 103.

Please amend paragraph [0089] beginning on page 55, as follows:

[0089] In the mediation-service management table 1034 there is held the following pieces of information for each mediating apparatus to be used.

a) IP address or host name of the mediating apparatus: IP address of the mediating apparatus.

b) Authentication scheme with the mediating apparatus (SPKI scheme, PKI scheme, challenge-response scheme, key-sharing scheme, etc.)

c) Name of certificate or the like for authentication (refer to the certificate/secret data corresponding to the authentication scheme).

In the mediation-service authentication information table 1035 there are held such pieces of information as listed below.

Please amend paragraph [0090] beginning on page 55, as follows:

[0090] a) Various certificates that are used for ~~client~~ authentication of VPN gateway unit by the VPN client unit (SPKI certificate, PKI certificate, password, common key, etc.),

b) Certificates that are used for authentication of the mediating apparatus ~~by the server~~ (SPKI certificate, PKI certificate, password, common key, etc.)

In the tunneling/protocol configuration management table there are held the following pieces of information for each tunnel to the VPN client unit.

a) IP address of the tunnel starting point (IP address given to the VPN client unit from the network).

Please amend paragraph [0093] beginning on page 56, as follows:

[0093] ii) Routing information to be posted to VPN client unit.

c) Packet filtering condition (which limits accessible services)

d) Range of private IP addresses deliverable to VPN client unit.

The VPN gateway unit 103 provides a secure communication channel to the mediating apparatus 104 by use of the mediation service management information table 1034 (step 31) and the mediation-service authentication information table 1035 (step 32), and issues a VPN access mediation request ~~(steps S1-S3)~~ (step S1). For example, upon authentication of the VPN client unit 101, the mediating apparatus 104 sends a VPN access mediation notice to the VPN gateway unit 103 ~~(step S4)~~ (step S5). The notice information (IP address IPADDRESS_A1 of the VPN client unit 101, common key KEY_AB, attribute information ATTRIBUTE_A1, etc.) is stored in the tunneling/protocol configuration management table 1036. Based on the attribute information, the VLAN 121 to be accommodated is determined, and the VLAN name "Personnel Division VLAN" is also stored in this table ~~(step S5)~~ (step S33). In this instance, the VPN client unit 101 is notified that it has the attribute information (VLAN Personnel Division) as shown in Fig. 20. Accordingly, it is determined that VLAN to accommodate the tunnel from the VPN client unit 101 is "Personnel Division VLAN."

Please amend paragraph [0094] beginning on page 57, as follows:

[0094] Upon issuance of a VPN tunnel set-up request from the VPN client unit 101 ~~(step S6)~~ (step S19), the VPN gateway unit refers to the tunneling/protocol configuration management table 1036 ~~(step S7)~~ (step S34), then performs predetermined authentication/encryption, after which it refers to the VLAN configuration management table 1037 of the corresponding VLAN ~~121(step S8)~~ 121 (step S35), then selects unused one of private IP addresses deliverable to the VPN client unit 101, and posts it to the VPN client unit 101, together with network configuration management information (addresses of the gateway, DNS, the WINS server, and so on). In this instance, the private IP address of the VPN client unit 101 is delivered from the address table of the personnel division VLAN. Also, network configuration management information on the gateway, DNS, etc. is posted from the personnel division VLAN.

Please amend paragraph [0095] beginning on page 58, as follows:

[0095] Upon arrival of a VPN-destined data packet at the VPN gateway unit through the above-mentioned tunnel from the VPN client unit 101, it is subjected, with reference to the VLAN configuration management table 1037 (step S36), to filtering based on the filter condition of VLAN having accommodated therein the tunnel, thereafter being transferred to the VLAN ~~(step S10)~~ (step S37). Besides, filtering for each tunnel may be additionally set using attribute information. Similar processing is also carried out for the request from the VPN client unit 102. In the case of disconnecting the tunnel, the corresponding entry is removed from the tunneling/protocol configuration management table 1036, and the private IP address assigned to the VPN client unit is returned to an address pool of the VLAN concerned. As described above, according to the present invention, the mediating apparatus stores information (access control list) that is used to establish a remote-access VPN by an arbitrary tunneling protocol, such as IPsec or L2TP, between each of the VPN client unit connected to the IP network and the VPN gateway unit, and an arbitrary communication unit connected to the local area network placed under the management of the VPN gateway unit. This information contains the private IP address assigned to the communication unit.